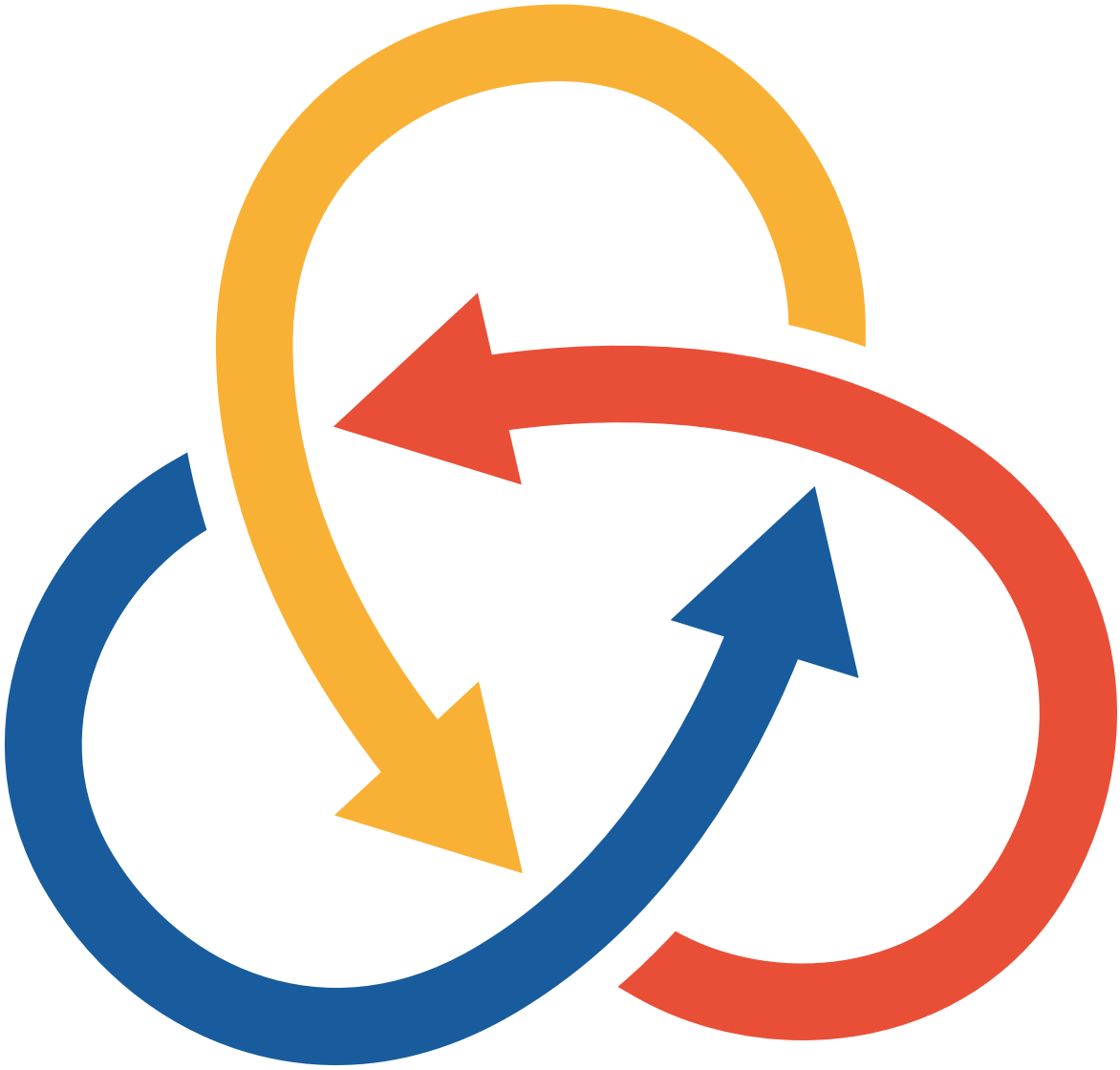
HOW CAN COMPETITION POLICY AND PRIVACY PROTECTION POLICY INTERACT?



BY GIULIANA GALBIATI & HENRI PIFFAUT[1]

1 Giuliana Galbiati is an adviser to the president of the Autorité de la concurrence. Henri Piffaut is a vice president at the Autorité de la concurrence. The views expressed in this article are those of the authors and do not represent those of the French Autorité de la concurrence.

CPI ANTITRUST CHRONICLE DECEMBER 2022

Visit www.competitionpolicyinternational.com for access to these articles and more!

HOW CAN COMPETITION POLICY AND PRIVACY PROTECTION POLICY INTERACT?

By Giuliana Galbiati & Henri Piffaut

While some initially argued that privacy was distinct and independent from competition enforcement, market realities and digitization have since then forced regulators to reflect upon how the two policies can be interrelated and increase their coordination efforts. Regulations like GDPR have rebalanced the asymmetry between platforms and users enabling privacy protection to become a relevant competition parameter. This paper examines how to best inform competition policy of privacy issues. It does so by distinguishing between mandated privacy protection and higher levels of protection and then between situations where privacy is a competition parameter and those where it is not. In all instances, exchanges with privacy regulators would help the competition agency determination.

I. WHY COMPETITION POLICY IS LIKELY TO INTERACT WITH OTHER PUBLIC POLICIES, AND WITH PRIVACY PROTECTION IN PARTICULAR

The perception of the interaction between competition policy and privacy protection has significantly evolved in recent years. While some initially argued that privacy was a distinct and complex issue and that competition enforcement should look the other way, market realities and digitization have since then forced regulators to reflect upon how the two policies can be interrelated and increase their coordination efforts. Regulations like GDPR try to give substance to privacy rights through definition of mandated levels of protection and consent. With the ensuing decrease in the asymmetry between platforms and users, privacy protection can become a relevant competition parameter. The question is then how to best inform competition policy of privacy issues. This paper examines possible answers.

Finding workable intersections between competition policy and other policies is not new. Just recently, there have been in-depth exchanges between EU competition authorities, including the Autorité de la concurrence (the "Autorité"), on how we can support the objectives of the European Green Deal in the framework of competition law. The European Commission's (the "Commission" or the "EC") revised HBER guidelines, which will include a specific chapter on sustainability agreements, as well as the revised guidelines on "State Aid for climate, environmental protection and energy 2022"[2] are concrete steps forward in this area. Even on the much-debated relationship between competition and industrial policies, there are several examples showing that the two can usefully complement each other. The recent hydrogen investment project known as IPCEI 2, approved by the Commission under state aid rules in July 2022, shows that it is possible to implement a modern industrial policy (here to strengthen Europe's position as a leading region for the hydrogen industrial transformation) while bringing competition on a newly created market. In fact, it could be argued that it is consubstantial to competition policy to interact with other policies that affect the competitive process.

In France, the legal framework has been designed to take into account the need for interaction between different policy objectives and regulators. The parliament, the government as well as sector regulators may or must (depending on circumstances) seek the opinion of the Autorité when legislative reforms or regulatory texts relating to competition are being prepared, or to explore ways of improving the competitive functioning of a sector or of specific geographical areas.

Conversely, in the antitrust area, the Autorité has a legal obligation (under article R.463-9 of the French commercial code) to consult sectoral regulators, by sending to them, when relevant, formal complaints or *ex-officio* decisions to open an investigation. Regulators may provide comments within two months. The Autorité has frequently used this mechanism in cases where privacy considerations were particularly relevant, as in the *Apple ATT* case (see below) with the CNIL, the French data protection regulator. As regards merger control, the legal obligation to consult sectoral regulators only applies with respect to the media industry (ARCOM)[3] and the banking and insurance industry ("ACPR")[4] in phase 2 proceedings. Of course, case teams always have the possibility to informally consult the data protection regulator in both phase 1 and phase 2 proceedings, as was recently done in the *TF1/M6* TV merger case.[5]

Beyond the enforcement of cases, we are witnessing a general movement towards the strengthening of cooperation between competition and privacy regulators. For instance, in the UK, the data protection authority, the ICO, and the CMA issued a joint statement in May 2021, presenting their common views on the relationship between competition and data protection in the digital economy. They emphasized the complementarity of the two regulatory frameworks, and affirmed their willingness to work together to find appropriate regulatory solutions.[6] This is notably the case in their joint review of *Google Chrome privacy sandbox* (see below). In France, where formal cooperation is already significant in both the advisory and enforcement frameworks, the Autorité and the CNIL have also engaged in other types of interaction, including presentations to the respective boards, cross-trainings of the investigation teams and joint workshops.

2 Communication from the Commission, Guidelines on State aid for climate, environmental protection and energy 2022, 2022/C 80/01, published in the OJEU on February 18, 2022.

3 Article 41-4, loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication.

4 Article L612-22, French Code monétaire et financier.

5 Autorité de la concurrence, press release, *TF1/M6: The Autorité de la concurrence takes note of the decision to withdraw its planned acquisition*, September 16, 2022.

6 "Competition and data protection in digital markets: a joint statement between the CMA and the ICO," 19 May 2021: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/987358/Joint_CMA_ICO_Public_statement_-_final_V2_180521.pdf.

As President Coeuré recently pointed out before the board of the CNIL, while the objectives pursued by competition law and privacy regulation differ, the two regulatory frameworks nevertheless present a certain convergence, in that they are ultimately implemented for the benefit of consumers.[7]

On the one hand, competition policy aims to guarantee the conditions for free and undistorted competition between companies, by promoting innovation, diversity of supply and attractive prices. It should be stressed that the role of competition policy is somewhat special in that its policy objective is very broadly defined and potentially may intersect with any public policy that may have an impact on consumers or companies' behaviors. It is also specific in that the responsibility for enforcement and policy has been granted to an independent entity, at least in Europe and in France. Other public policies have in general a more focused objective and sometimes rely only on the judicial system for their enforcement, as opposed to a dedicated agency.

On the other hand, privacy policy aims at ensuring personal data protection, defining when, how and to what extent information about a person can be collected, processed, and communicated by and between undertakings. Privacy law, such as the GDPR, provides basic protection to individuals and data subjects, and affords rights to better control their personal data. Most jurisdictions operate a consent-based regime, which provides consumers with the ability to control how their data are collected and used by agreeing or withholding their consent.

However, companies design the choice architecture that leads to such consent, and this may influence the extent of the possible choice. In addition, in some jurisdictions, data protection legislation, as in the case of the GDPR, confers other rights, including the right to data portability. Again, the reality of that right will depend in part on companies' behavior and on privacy regulatory design. Both the relevant information on privacy and data portability can have significant effects on competition. Such legislation and implementing measures create a space where, theoretically, individuals can exercise a choice over the level of protection provided on their personal data and also allows comparison between undertakings on the level of protection offered. By doing so it opens privacy protection to become a genuine competition parameter.

The level of privacy protection would become a relevant competition parameter once meeting the legal requirements with regards to privacy protection (what can be called "mandated privacy protection"). Since these levels of protection have been mandated, all players on the market shall equally comply with the same requirements. However, if there are discretionary elements in how to implement the protection of basic privacy, there can be competition among different players on that basis. In addition, competition plays fully for the provision of privacy protection that goes beyond mandated levels. There is however the caveat of who would decide the mandated level has been achieved or the choice architecture is a real one. If the regulatory setting does not allow clear and quick conclusions on these, there would be a need for determination in a competition enforcement case.

Conversely, it could also be argued that lack of implementation of a privacy regulation could be seen as an infringement under both competition law (for instance where it constitutes an abuse of dominance) and privacy regulation. The most striking example of this scenario is the 2019 Facebook case before the Bundeskartellamt (discussed below). The Google related rights decisions by the Autorité[8] - even though they fall outside the scope of privacy regulation - are also a relevant example of how infringing or circumventing a regulation (in this case the European directive on related rights and the implementing French regulation) can possibly result in a violation of competition law.

Moreover, provisions such as data portability may lower (at least theoretically) switching costs for individuals if they want to change providers. "Theoretically » because for portable data to be useful, it should follow some standards in definition and format. It does not seem that we are yet there."[9] Conversely, the provision of privacy protection can become a way to raise barriers to entry. A company that controls a bottleneck in providing access to competitors to a market could structure the choice architecture for individuals to grant consent in such a way that individuals would be disinclined to grant consent. This is basically the claim of complainants asking for interim measures in 2020 in the *Apple ATT* case (the case has continued its life since then and this article does not take any stance on facts or law in that regard).

7 Speech of the president of the Autorité de la concurrence, Benoît Coeuré, before the CNIL, June 2, 2022, https://www.autoritedelaconcurrence.fr/sites/default/files/2022-06/20220608-CNIL-discours_0.pdf.

8 Décision n° 20-MC-01 du 9 avril 2020 relative à des demandes de mesures conservatoires présentées par le Syndicat des éditeurs de la presse magazine, l'Alliance de la presse d'information générale e.a. et l'Agence France-Presse ; décision n° 21-D-17 du 12 juillet 2021 relative au respect des injonctions prononcées à l'encontre de Google dans la décision n° 20-MC-01 du 9 avril 2020 ; décision n° 22-D-13 du 21 juin 2022 relative à des pratiques mises en œuvre par Google dans le secteur de la presse.

9 Case T-604/18, judgment of the General Court, 14 September 2022, §184: "In this regard, first, it should be observed that user loyalty to Android was not attributable, according to the Commission, solely to the quality of the OS. As the Commission indicated on the basis of the statements of OEMs cited in recitals 524 and 534 of the contested decision, the high degree of user loyalty to Android could also be accounted for by the difficulties users encountered in porting personal data or by the need to repurchase apps. In particular, as noted inter alia by one of those OEMs, users get used to the way their smart device works and do not want to relearn a new system (see recital 534(3) of the contested decision). User loyalty could not, however, be attributable to the quality of the OS alone, as the Commission stated in recital 488 of the contested decision, since many users were using Android versions that had not been updated."

Apple had announced in June 2020 its intention to implement a mechanism called ATT (App Tracking Transparency) by September 2020. This mechanism displays a pop-up window which requires the explicit consent of the iPhone user before any use of their "Identifier for Advertisers." This unique identifier allows online advertising companies to track users' activity on different websites or mobile apps, for the purposes of targeted advertising. The complaint filed before the Autorité asking for interim measures argued that the ATT prompt would constitute an abuse of a dominant position because it would be neither necessary nor proportionate to achieve Apple's objective of protecting users' privacy. The Autorité rejected the request for interim measures but decided to investigate the merits of the case.[10]

While it is therefore apparent that competition and privacy policies interact in many instances, the relationship between the level of privacy protection and the level of competition is not necessarily obvious. Indeed, competition policy seeks to address a market failure according to which firms may tend, collectively or unilaterally, to abuse market power and deprive consumers from the benefits of competition. In this context, offering a high level of privacy protection (mandated or not) may be a way to increase barriers to entry for competitors, as illustrated by the debate over Apple's introduction of ATT. Alternatively, a lower level of privacy protection may enable a firm to increase its returns over a dataset across markets, and may be tested once a company faces lower competitive constraints.

A consequence of this is that competition enforcement is not as efficient a tool to address privacy issues as privacy regulation. For example, the design of competition remedies usually looks at the root cause of market power that created the ability and incentive for the undertakings concerned to restrict competition. If an agreement or a unilateral action were found to restrict competition because they materially decreased privacy protection (while still meeting mandated obligations), a cease and desist order would be efficient to eliminate the ability to restrict competition only if accompanied by a monitoring akin to dedicated regulation; it would however be difficult to eliminate the incentive to behave in this harmful way, since it does not necessarily find its source in market power.

II. SCENARIOS WHERE COMPETITION POLICY AND PRIVACY POLICY ARE INTERRELATED/ INTERDEPENDENT

We identified three possible approaches in order to take into account privacy considerations in a competition law assessment: consider the two policies as autonomous and ignore; acknowledge that there is a coordination issue but defer its resolution to the privacy regulator and then adjudicate on the competition matter; or take an informed stance on the privacy issue that can serve as a basis for the competition assessment.

As for the first, the old stance claiming that, since each public policy has its own objectives, they should more or less ignore each other does not seem sustainable anymore. This is the approach that the European Commission followed in its 2008 review of the *Google/DoubleClick* merger in the online advertising industry, where one of the three non-horizontal theories of harm concerned the combination of Google and DoubleClick's data collection. The decision states that the Commission's review was limited to assessing whether the transaction would not impede effective competition, and was without prejudice to other obligations imposed onto the parties in the area of privacy and data protection.[11]

This was consistent with the Court ruling in the *Asnef Equifax* case, where the Court had to examine whether agreements concluded for the purpose of setting up credit information registers in Spain were potentially restrictive of competition and whether they could be exempted on the basis of Article 101(3). When examining the existence of a restriction of competition, the Court observed that it was not relevant to take into account privacy considerations in the context of the competition assessment: *"any possible issues relating to the sensitivity of personal data are not, as such, a matter for competition law, they may be resolved on the basis of the relevant provisions governing data protection," before adding however that it was "apparent from the documents before the Court that, under the rules applicable to the register, affected consumers may, in accordance with the Spanish legislation, check the information concerning them and, where necessary, have it corrected, or indeed deleted."*[12]

Similarly, in the 2014 F*acebook/WhatsApp* case, the Commission assessed the possible concerns associated with the combination of the two entities' datasets to determine whether it could constitute an obstacle to competition in the online advertising market. It pointed out however that it *"analysed potential data concentration only to the extent that it is likely to strengthen Facebook's position in the online advertising market or in any sub-segments thereof. Any privacy-related concerns flowing from the increased concentration of data within the control of*

10 Décision n° 21-D-07 du 17 mars 2021 relative à une demande de mesures conservatoires présentée par les associations Interactive Advertising Bureau France, Mobile Marketing Association France, Union Des Entreprises de Conseil et Achat Media, et Syndicat des Régies Internet dans le secteur de la publicité sur applications mobiles sur iOS.

11 Case M.4731 – *Google/DoubleClick*, March 11, 2008, paragraph 368.

12 Case C-238/05, judgment of the Court, November 23, 2006, *Asnef-Equifax, Servicios de Información sobre Solvencia y Crédito, SL v. Asociación de Usuarios de Servicios Bancarios (Ausbanc),* paragraph 63.

Facebook as a result of the Transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules."[13]

With the digitization of the economy, the use of personal data has become pervasive. The role of data and consequently consumers' preferences with regard to their privacy cannot anymore be separated as a rule from a competition assessment. Today most industries rely at least to some extent on data. It can be at the stage of the production process, at the commercial stage, for instance to improve marketing, or in the way products or services are sold. Digitization has also enabled the development of platform businesses.

A platform can be seen as an enabler for transactions between sides to take place. For the match to take place and then the transaction to be completed, a platform relies on data provided by both sides. From a competition standpoint, the accumulation of data can constitute an important source of market power. Very often such datasets may include personal data and therefore their use may raise privacy protection issues. This is even more the case when the platform includes a "data side," i.e. uses or grants access to personal data to provide targeted advertisement. In addition, as discussed earlier, the adoption of privacy protection legislation based on information of consumers and seeking their consent has led to consumers being better able to compare and express preferences in relation to levels of privacy protection.

The second approach is akin to the solution adopted in IP matters: a competition authority may find a patent to be obviously invalid but may not take a stance on validity or infringement beyond finding that there is uncertainty on the outcome of disputes. Since most conflicts in IP are adjudicated through court proceedings, such an approach may make sense. In privacy matters, where a dedicated regulator has been attributed some monitoring powers, this approach would present the drawback that available expert opinion would not be sought in the course of competition proceedings.

The third approach would go further than the second in allowing to make a finding based on exchanges with the privacy regulator. That is the approach that the Bundeskartellamt followed in its *Facebook* case, where it considered that imposing on users the aggregation of their data in violation of the provisions of the GDPR constituted an exploitative abuse of Facebook's dominant position. The legality of this approach is one of the questions put to the European Court of Justice in the request for a preliminary ruling from the Higher Regional Court of Düsseldorf. Advocate General Rantos rephrased that question in the following way: "[may] *a competition authority (…) examine, as an incidental question, the compliance of the practices under investigation with the GDPR rules, while taking account of any decision or investigation of the competent supervisory authority on the basis of the GDPR, informing and, where appropriate, consulting the national supervisory authority"*?[14] His proposed answer is "yes," noting though that the competition authority could "possibly" wait for the outcome of the privacy regulator investigation and its findings could not bind the regulatory authority.

In the following we first examine to what extent privacy could be taken into account when it is not considered as a competition parameter and then look at the situation where it would be a competition parameter.

III. WHERE PRIVACY PROTECTION IS NOT A RELEVANT COMPETITION PARAMETER FOR THE ASSESSMENT OF A PRACTICE, BUT…

The conduct in question (negatively) affects both competition (in terms of prices, quality, innovation, etc.) and privacy. Even where privacy protection would not be a competition parameter, a given conduct or merger could still affect in parallel both competition and privacy. In this scenario, the competition agency should focus its efforts on solving the competition issue; however this might also have an impact on privacy considerations, and it would not seem appropriate that the two policies ignore each other. The definition of appropriate measures in both areas should somehow be coordinated.

For instance, in its *Google/Fitbit* merger decision[15] the Commission looked at the impact of the aggregation of Fitbit's health and fitness user data with Google's existing datasets. It found no evidence that privacy was a parameter of competition for wearable devices and accordingly, did not include privacy in its substantive assessment of the transaction. In addition, it presumed that Google and Fitbit would lawfully combine their databases under privacy law. Should such presumption prove to be incorrect, the *"effects of the transaction […] would be the same, but the parties remain accountable for any breach of GDPR or the e-Privacy Directive."* Obviously, this assessment relies on the assumption that privacy would continue in the future not to be a parameter of competition in that field.

13 Case M.7217 – *Facebook/WhatsApp*, October 3, 2014, paragraph 164.

14 C-252/21, Opinion of Advocate General Rantos, September 20, 2022, *Meta Platforms and Others*, paragraph 33.

15 Case M.9660 – *Google/Fitbit,* December 17, 2020.

The conduct in question is pro-competitive but negatively affects privacy protection. When a conduct or merger is pro-competitive, competition law does not apply, and it would be for the privacy regulator to address any issue under privacy law in order to evaluate whether privacy regulation has been violated. It could be argued that the privacy regulator should however make sure that any negotiated settlement over privacy protection would not lead to restrictive effects on competition and limit the *effet utile* of competition law.

The conduct in question restricts competition but is compliant with privacy regulation and/or positively affects privacy protection. Alternatively, when a conduct or merger restricts competition but at the same time impacts positively privacy protection, there is no balancing exercise to undertake among several competition parameters to assess the effect on competition, since privacy protection is not a competition parameter. A balancing exercise could however take place under Article 101(3) or as a second step in the analysis under Article 102. The first condition under Article 101(3) states that the agreement or concerted practice in question should contribute to improving the production or distribution of goods or to promoting technical or economic progress.

That would seem to include a public policy objective such as protecting privacy. This is dependent on checking whether the envisaged measures do really enhance privacy protection which may require expert opinion. Privacy protection would likely be accepted to fulfill the second condition of Article 101(3), i.e. that the agreement should allow consumers a fair share of the resulting benefit. The third and fourth conditions, related to the indispensable nature of the restriction and the fact that the agreement shall not eliminate competition in respect of a substantial part of the products in question, would amount to a proportionality test whereas the undertakings concerned would have to show that there are no other ways to achieve the same objective that would less restrict competition. A similar exercise could take place under Article 102. Usually solving such an issue would cause a variation in the level of privacy protection. This is discussed in the next scenario.

The conduct in question restricts competition and the measures envisaged to remedy the competition issue may involve privacy protection considerations. The last possible scenario that we identified would be when a conduct or merger would restrict competition (with no plausible justification under privacy protection) and solving the competition issue could lead to a variation in the level of privacy protection. Clearly the competition agency could not impose measures that would violate privacy protection rules. However, when the variation in privacy protection would be negative while not infringing privacy rules, what should the competition agency do?

First of all, it should be underlined that compliance or not with privacy rules may not be obvious to assess. In that case, it would seem desirable, save for confidential information, that competition agency would consult with the competent privacy protection agency to check that aspect. As mentioned above, such consultation rules exist under French law, however, in the antitrust area, it is only required by law when the formal complaint or the decision to open an *ex-officio* investigation relate to sectors falling within the areas of expertise of the CNIL. In addition to the fact that privacy regulation can hardly be regarded as a sector, it may not be easy to know, at that early stage of the proceeding, that the measures that will later on be envisaged to remedy the competition issue will have an impact on privacy protection rules. In this respect, such scenario does not necessarily entail a mandatory consultation of the CNIL, but the investigation team might still wish, at the remedy stage, to contact the data protection agency on an informal basis.

Assuming now that the variation in privacy protection caused by the resolution of the competition issue would not lead to compliance issues, the question remains to what extent the competition agency should, ceteris paribus, favor a solution that would harm the least privacy protection. After all, the European legislator has granted a special status to privacy protection.

In this context, privacy rules may act as an external constraint on the design of merger remedies. Access to a dataset could both lower barriers to entry and risk running contrary to privacy rules. For instance in *Google/Fitbit*, the EC conditioned clearing the transaction on Google's commitment to provide users with an effective choice to: (i) grant or deny the use of certain Fitbit data by Google services; and (ii) allow third parties' access to the data types made available in the Fitbit Web API, subject to certain privacy and security requirements. In France, the Autorité informally consulted the CNIL in its *Enerest/Electricité de Strasbourg* case[16], in order to ensure the compliance with privacy regulation of a data access commitment, whereby the parties (two historical suppliers of gas and electricity) committed to send every competitor that would request it the necessary customer information to design their own offers.

Similarly, in some conduct cases, the Autorité was constrained in remedying a restriction of competition because of privacy protection considerations. Two relevant French cases include the *GDF-Suez* case[17] and the recent EDF case,[18] both in the energy sector. In the first one, the

16 Décision n° 12-DCC-20 du 7 février 2012 relative à la prise de contrôle exclusif d'Enerest par Electricité de Strasbourg, see §89.

17 Décision n° 14-MC-02 du 9 septembre 2014 relative à une demande de mesures conservatoires présentée par la société Direct Energie dans les secteurs du gaz et de l'électricité (interim measures decision); décision n° 17-D-06 du 21 mars 2017 relative à des pratiques mises en œuvre dans le secteur de la fourniture de gaz naturel, d'électricité et de services énergétiques (decision on the merits).

18 Décision n° 22-D-06 du 22 février 2022 relative à des pratiques mises en œuvre par la société EDF dans le secteur de l'électricité.

CNIL was formally consulted by the Autorité under article R.463-9 of the French commercial code in light of the data-related concerns expressed by a competitor (Direct Energie) in its formal complaint and with respect to the interim measures that the Autorité was considering.

These measures consisted of the incumbent granting its competitors an access to some of the data it had collected as a provider of regulated offers, in order to ensure effective competition on a separate market that had recently been opened to competition. The CNIL provided relevant information with respect to the data that could be shared as well as the process that had to be put in place to collect customers' approval to such data sharing. In the 2022 EDF case, EDF decided to settle an abuse of dominance case and offered a series of commitments, including the sharing of its customer file on the relevant market with alternative electricity suppliers who requested it. The CNIL was informally consulted on the commitments' proposal, and it is apparent from their final drafting that privacy protection considerations were taken into account by EDF.[19]

It is worth stressing that the design and monitoring of remedies that would involve requiring consent for privacy protection reasons would need to pay particular attention to the choice architecture followed when seeking consent. If not properly designed these remedies could lead to additional barriers to entry.

IV. WHERE PRIVACY PROTECTION IS A COMPETITION PARAMETER

It is now widely accepted that privacy protection (beyond its mandated level) has become a possible competition parameter. One of the early manifestations of this was Facebook's growth at the expense of MySpace. At the time, Facebook advertised its services as better able to protect users' privacy than that of MySpace, the incumbent.

In its recent judgement on the Commission's decision in the *Google Android* case, the General Court acknowledged that *"variables other than technical quality, such as the protection of privacy (…) also play a role"* (para 578). It has also been argued that infringement of privacy regulation could amount to a competition law infringement (see discussion above with regard to the 2019 Facebook case before the Bundeskartellamt).

Consumers could therefore consider privacy protection as a relevant competition parameter, in particular where players can exercise discretion in deciding how to implement privacy regulation or where they decide to go beyond what is legally required. In a way equivalent to the assessment of impact on quality, the effect on competition of a certain conduct or merger should then consider the impact on privacy protection.

Accepting that privacy protection would amount to a competition parameter leads to some balancing exercise of the effects of an agreement, a unilateral action or a merger on that parameter and other parameters such as quality, quantity, price, etc. It is the outcome of this balancing that would lead to the conclusion that there is a restriction of competition. Whereas in the case of two independent policies, the balancing would take place in the form of a proportionality test (if there was first a restriction of competition), here it would be a more in-depth analysis at the first stage of the competition law assessment, i.e. under Art 101(1) or Art 102 prior to the examination of efficiency or objective justifications. However, there would still be an assessment at the second stage of the competitive assessment, as discussed above. Several scenarios could be envisaged in this context.

The conduct in question would harm certain parameters of competition while leading to an increase in privacy protection (beyond what is mandated by law). This scenario would need to pass a first stage analysis before the proportionality assessment described above: the competition agency would have to determine whether the overall effect would be restrictive or not. This would be an evaluation similar to that of ancillary restraints.

As stated in *MasterCard*, a restriction is ancillary when an operation that is not anticompetitive in nature, would be impossible to carry out in the absence of the restriction in question. It would not be enough if the operation were more difficult to implement or less profitable without the restriction.[20]

The conduct in question would harm several competition parameters*, including privacy.* In this scenario, where a given practice would therefore infringe competition law at the first stage of the analysis, the competition authority and the data regulator would have to coordinate very closely if only to determine the level of harm on privacy and whether mandated privacy is involved. In the antitrust area, it is conceivable that the competition agency would decide to let the privacy regulator deal first with the issue. However, that would require two prerequisites: that the issue is mostly one of privacy protection and that the regulator would be competent, i.e. that the behavior would likely infringe privacy law. Such preliminary finding would mean that the two agencies would early on discuss the issue. In practice it seems unavoidable that the compe-

19 See for instance pages 3 to 7 of EDF's commitments and Annexes 1 and 2 attached to the decision.

20 C-382/12 P, judgment of September 11, 2014, *MasterCard and Others v. Commission*, paragraph 91.

tition agency would at some point have to take position, also in light of the fact that other competition parameters would be affected alongside privacy.

In the case of merger control, a competition agency would have no discretion to let a regulator deal with privacy issues when these are a competition parameter. In *Facebook/WhatsApp*,[21] the Commission found that privacy was an important parameter of competition in relation to consumer communication services. In *Microsoft/LinkedIn*, the Commission found that privacy was a *"significant factor of quality"* and therefore an important parameter of competition and "*driver of consumer choice."* If the market for PSN services reached a "tipping point" in favor of LinkedIn after its combination with Microsoft, the Commission noted that this would restrict consumer choice in relation to privacy protection, an *"important parameter of competition"* according to its investigation, when choosing a PSN.[22] In that case the Commission posited that one effect of the merger would be a decrease in competition constraints from other players with better privacy protection. There was no examination of the relationship between market structure and incentive to protect privacy.

When privacy is a competition parameter, but the issue is mostly one distinct from privacy protection or when the effect on privacy is outside the scope of mandatory actions. In these scenarios the competition agency would need to make an assessment that would also cover privacy protection. Here again, a mechanism that would seek views from the privacy regulator over the effect of the behavior on mandated or not mandated protection and possible remedies over privacy protection would seem advisable. In addition, the developments above on how to solve the competition issue while minimizing negative effects on privacy protection remain relevant.

The UK CMA's review of Google's privacy sandbox, in coordination with the ICO, is a relevant example for cooperation between the two regulators.

Google, with its proposed "privacy sandbox," intended to change its web browser in order to address privacy concerns by replacing cross-site tracking of users (notably through cookies) with a set of alternative tools. The CMA was concerned that Google's privacy sandbox would lead to unequal access for third parties to the functionality associated with user tracking, Google "self-preferencing" its own ad tech providers and ad inventory, and the imposition of unfair terms on Chrome's web users. In addition, the ICO had its own concerns over the impact on data protection law and privacy outcomes for individuals.

The CMA explained that in assessing concerns and negotiating and designing remedies it had been "working closely" with the ICO. In addition, since the remedies were dynamic in nature, it would continue to consult the ICO to ensure that both privacy and competition concerns were addressed as the proposals were developed in more detail.

V. CONCLUSION

It is now clear that competition and privacy policies are interrelated. Against this background, there is a need for coordination to maximize outcomes of both policies. However, these policies operate within two distinct regulatory settings (on material competences and geographies) and that makes such coordination complicated: there is a risk that perceived regulatory failure on the privacy side be filled in by competition law enforcement.

It is also important to bear in mind that in Europe other legislative tools will be added to the existing regulatory framework in the coming months, which may increase the degree of complexity in dealing with this issue. The obligations imposed by the Digital Markets Act, see for instance article 5(2) of the regulation, will also play a key role in regulating the illegal practices of digital platforms with respect to the collection, combination, and use of personal data. The impact of the proposed Data Act, which aims to increase the fair use and sharing of data across all economic sectors, will also need to be taken into account.

Finally, one should not ignore the impact of evolving technology which may upend interaction between privacy and competition notably when access to datasets and portability are concerned.

21 Case M.7217 - *Facebook/WhatsApp*, October 3, 2014, paragraphs 87, 102 and footnote 79.

22 Case M.8124 - *Microsoft/LinkedIn*, December 6, 2016, paragraphs 349-351.

CPI COMPETITION POLICY® INTERNATIONAL

CPI Subscriptions

CPI reaches more than 35,000 readers in over 150 countries every day. Our online library houses over 23,000 papers, articles and interviews.

Visit competitionpolicyinternational.com today to see our available plans and join CPI's global community of antitrust experts.